Mercredi 15 Février 2017

Structures-Arithmétique

Durée : 4 heures

Jean le Rond D'Alembert(1717-1783)

Mathématicien et philosophe français. Il fût abondonné par sa mère, le deuxième jour de sa naissance, devant la porte de la chapelle *Saint-Jean-le-Rond*. Lauréat de l'École de Droit, refusant de s'inscrire au barreau, il entreprit des études de médecine. Il commence ses premiers travaux scientifiques en astronomie. Ami de Voltaire, il était un habitué des salons parisiens. D'Alembert est considéré comme un théoricien de la musique. Ses études de la vibration des cordes font de lui l'un des fondateurs de la physique mathématique. Il est aussi pour avoir dirigé l'Encyclopédie pour ses contributions en mathématiques.

Questions de Cours :

1. Rappeler les propriétés caractéristiques de :
   - i. Sous-groupe, sous anneau, sous-corps ;
   - ii. Sous-espace vectoriel, sous algèbre ;
   - iii. PGCD, PPCM.
2. Rappeler les énoncés des théorèmes suivants :
   - i. Bezout (version 1 et 2) ;
   - ii. Gauss

Exercice Application-Cours :

On considère la suite $(F_n)_{n\in\mathbf{N}}$ définie par les relations

$$F_0 = 0,\ F_1 = 1,\ \text{et } \forall n \in \mathbf{N}^\star,\ F_{n+1} = F_n + F_{n-1}$$

Les F_n sont des nombres entiers naturels appelés **nombres de Fibonacci**.

1. Montrez que pour tout entier naturel $n \in \mathbf{N}^\star$, $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$. Déduisez-en que F_n et F_{n+1} sont premiers entre eux.

2. Montrez que pour tout couple $(n,p) \in \mathbf{N} \times \mathbf{N}^\star$, $F_{n+p} = F_pF_{n+1} + F_{p-1}F_n$. Déduisez-en que

$$PGCD(F_n, F_p) = PGCD(F_{n+p}, F_p)$$

3. Démontrez finalement,

$$\forall (n,p) \in \mathbf{N}^2, \quad PGCD(F_n, F_p) = F_{PGCD(n,p)}$$

4. En déduire que F_n divise F_m si et seulement si n divise m

Problème 1 Convolution de suites réelles

$E=\mathbb{R}^{\mathbb{N}}$ désigne l'ensemble des suites réelles.

Pour $u\in E$, on note $u(n)$ au lieu de u_n le terme d'indice n de la suite u.

Pour $u,v\in E$, on appelle somme des suites u et v, la suite $u+v\in E$ définie par :

$$\forall n\in\mathbb{N},(u+v)(n)=u(n)+v(n).$$

On sait que la loi de composition interne $+$ sur E ainsi définie munit E d'une structure de groupe commutatif d'élément nul égal à la suite nulle notée 0.

Pour $u,v\in E$, on appelle convolé de la suite u par la suite v, la suite $u\star v\in E$ définie par :

$$\forall n\in\mathbb{N},(u\star v)(n)=\sum_{k=0}^{n}u(k)v(n-k).$$

La loi de composition interne $\star$ sur E ainsi définie est appelée produit de convolution de suites réelles.

1.a Montrer que $\star$ est commutative et associative.

1.b On note ε la suite réelle définie par $\varepsilon(0)=1$ et $\forall n\in\mathbb{N}^*,\varepsilon(n)=0$.
Etablir que ε est élément neutre pour $\star$.

1.c Montrer que $\star$ est distributive sur $+$.

1.d Que dire de la structure $(E,+,\star)$?

2.a Soit $\rho\in\mathbb{R}$ et u la suite réelle définie par $\forall n\in\mathbb{N},u(n)=\rho^n$.
Montrer que l'élément u est inversible et déterminer son inverse.

2.b On note $F=\mathbb{R}^{(\mathbb{N})}$ l'ensemble des suites réelles nulles à partir d'un certain rang.
Montrer que F est un sous-anneau de l'anneau $(E,+,\star)$.

2.c Soit $f:E\to E$ définie par : $\forall u\in E$, la suite $f(u)\in E$ est donnée par $\forall n\in\mathbb{N},\big[f(u)\big](n)=(-1)^n u(n)$.
Montrer que f est un automorphisme involutif de l'anneau $(E,+,\star)$.

3. On se propose maintenant de déterminer les éléments inversibles de l'anneau $(E,+,\star)$.

3.a Soit u un élément inversible de l'anneau $(E,+,\star)$. Montrer que $u(0)\neq 0$.

3.b Inversement soit $u\in E$, tel que $u(0)\neq 0$. Montrer que u est inversible.

4. On se propose maintenant de justifier l'intégrité de l'anneau $(E,+,\star)$.
Soit $u,v\in E$ tels que $u\neq 0$ et $v\neq 0$.
On pose $p=\min\{n\in\mathbb{N}/u(n)\neq 0\}$ et $q=\min\{n\in\mathbb{N}/v(n)\neq 0\}$.

4.a Justifier l'existence de p et q.

4.b Montrer que $(u\star v)(p+q)\neq 0$.

4.c Conclure.

Problème 2 Entiers somme de deux carrés

L'objectif de ce problème est de déterminer quels sont les entiers naturels qui sont somme de deux carrés.

Notations :

$\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{C}$ désignent respectivement les ensembles des entiers naturels, des entiers relatifs et des nombres complexes.
On pose $\mathbb{Z}[i]=\{a+ib/a\in\mathbb{Z},b\in\mathbb{Z}\}\subset\mathbb{C}$ et $\mathbb{Z}[i]^*=\mathbb{Z}[i]\setminus\{0\}$.
Pour $z\in\mathbb{C}$, on pose $N(z)=z\overline{z}$.

Partie I :Présentation de l'anneau de $\mathbb{Z}[i]$

1. Présentation de l'anneau $\mathbb{Z}[i]$.

1.a Vérifier que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$ muni de l'addition et de la multiplication usuelles.

1.b Etablir que pour tout $u,v\in\mathbb{Z}[i]$, $N(uv)=N(u)N(v)$ et que pour tout $u\in\mathbb{Z}[i]$, $N(u)\in\mathbb{N}$.

1.c Un élément $u\in\mathbb{Z}[i]$ est dit inversible ssi il existe $v\in\mathbb{Z}[i]$ tel que $uv=1$.
Montrer que si u est inversible alors $N(u)=1$.
Déterminer alors l'ensemble, noté U, des éléments inversibles de $\mathbb{Z}[i]$.

2. Divisibilité dans l'anneau $\mathbb{Z}[i]$.
Soit $u,v\in\mathbb{Z}[i]$. On dit que u divise v dans $\mathbb{Z}[i]$, et on note $u\mid v$, ssi il existe $s\in\mathbb{Z}[i]$ tel que $v=su$.

2.a Soit $u,v,w\in\mathbb{Z}[i]$. Etablir l'implication que si $u\mid v$ et $v\mid w$ alors $u\mid w$.

2.b Soit $u,v\in\mathbb{Z}[i]$. Etablir que si $u\mid v$ et $v\mid u$ alors $u=\pm v$ ou $\pm iv$.

2.c Soit $u,v\in\mathbb{Z}[i]$. Montrer que si u divise v alors $N(u)$ divise $N(v)$ dans $\mathbb{Z}$.

2.d Déterminer les diviseurs de $1+i$, puis de $1+3i$ dans $\mathbb{Z}[i]$.

3. Division euclidienne dans $\mathbb{Z}[i]$.

3.a Montrer que pour tout $z\in\mathbb{C}$, il existe $u\in\mathbb{Z}[i]$ tel que $N(u-z)<1$.
Ce u est-il unique ?

3.b Montrer que pour tout $u\in\mathbb{Z}[i]$ et tout $v\in\mathbb{Z}[i]^*$, il existe $(q,r)\in\mathbb{Z}[i]\times\mathbb{Z}[i]$ tel que :
$u=vq+r$ avec $N(r)<N(v)$.
On pourra utiliser la division dans $\mathbb{C}$.

Partie II : Arithmétique dans $\mathbb{Z}[i]$

1. Soit $\delta\in\mathbb{Z}[i]$. On note $\delta.\mathbb{Z}[i]=\{\delta u/u\in\mathbb{Z}[i]\}$.
Montrer que $\delta.\mathbb{Z}[i]$ est un sous-groupe additif de $\mathbb{Z}[i]$.

2. Soit $u,v\in\mathbb{Z}[i]$ avec $u\neq 0$ ou $v\neq 0$. On note $I(u,v)=\{uz+vz'/z,z'\in\mathbb{Z}[i]\}$.

2.a Observer que u et v appartiennent à l'ensemble $I(u,v)$.

2.b Montrer que l'ensemble $A=\{N(w)/w\in I(u,v)\setminus\{0\}\}$ possède un plus petit élément $d>0$.

2.c Soit δ un élément de $I(u,v)$ tel que $N(\delta)=d$. Etablir que $I(u,v)=\delta.\mathbb{Z}[i]$.
On pourra exploiter la division euclidienne présentée en I.3b.

2.d Montrer que δ divise u et v puis que
pour tout $w\in\mathbb{Z}[i]$, on a l'équivalence : ($w\mid u$ et $w\mid v$) $\Leftrightarrow w\mid\delta$.
On dit que δ est un pgcd de u et v.

3. Soit $u,v\in\mathbb{Z}[i]$ avec $u\neq 0$ ou $v\neq 0$.

On dit que u et v sont premiers entre eux ssi le nombre δ défini en II.2.d appartient à $\{\pm 1,\pm i\}$.

Dans les questions 3.a et 3.b, on suppose que u et v sont premiers entre eux.

3.a Justifier qu'il existe $z,z'\in\mathbb{Z}[i]$ tel que $1=uz+vz'$

3.b Soit $w\in\mathbb{Z}[i]$. Montrer que si u divise vw alors u divise w.

4. Soit $u\in\mathbb{Z}[i]-\{0,\pm 1,\pm i\}$.

On dit que u est irréductible ssi ses seuls diviseurs sont $\pm 1,\pm i,\pm u$ et $\pm iu$.

4.a Soit $v\in\mathbb{Z}[i]$. On suppose que u irréductible et ne divise pas v.

Montrer que u et v sont premiers entre eux.

4.b Soit $v,w\in\mathbb{Z}[i]$. On suppose que u est irréductible et divise vw.

Montrer que u divise v ou divise w.

Partie III : Nombres somme de deux carrés

1. On note $\Sigma=\left\{a^2+b^2 / a\in\mathbb{Z},b\in\mathbb{Z}\right\}$.

1.a Montrer que $n\in\Sigma\Leftrightarrow\exists u\in\mathbb{Z}[i],n=N(u)$.

1.b En déduire que si $n,n'\in\Sigma$ alors $nn'\in\Sigma$.

2. p désigne un nombre premier strictement supérieur à 2.

2.a Montrer que $p\in\Sigma\Rightarrow p\equiv 1$ modulo 4.

Nous admettrons que l'implication réciproque est vraie (quoique loin d'être immédiate).

Ainsi $5=1^2+2^2$, $13=2^2+3^2$, $17=1^2+4^2$,... sont des éléments de Σ.

2.b Montrer que si p n'est par irréductible alors $p\in\Sigma$.

3. Soit $a,b\in\mathbb{Z}$ et $n=a^2+b^2\in\Sigma$. Soit $p\equiv 3$ modulo 4, un nombre premier diviseur de n.

3.a Montrer que $p\,|\,a+i.b$ dans $\mathbb{Z}[i]$.

3.b En déduire que p^2 divise n.

4. Etablir que les entiers naturels non nuls appartenant à Σ sont les nombres de la forme $n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_N^{\alpha_N}$ avec $p_1,p_2,\ldots,p_N$ nombres premiers deux à deux distincts et $\alpha_1,\alpha_2,\ldots,\alpha_N$ entiers naturels tels que :

$\forall 1\leq i\leq N$, $p_i\equiv 3$ modulo 4 $\Rightarrow\alpha_i$ est pair.

Mercredi 15 Février 2017

Structures-Arithmétique

Corrigé

Exercice Application-Cours :

Soit $(F_n)_{n\in\mathbf{N}}$ la suite définie par les relations $F_0 = 0$, $F_1 = 1$, et $\forall n \in \mathbf{N}^\star$, $F_{n+1} = F_n + F_{n-1}$.

1. Montrons par récurrence sur $n \in \mathbf{N}^\star$ que $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.

- **Initialisation :** pour $n = 1$, on a $F_2 \times F_0 - F_1^2 = 0 - 1 = -1$.
- **Hérédité :** soit $n \in \mathbf{N}^\star$ tel que $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$. Utilisons les relations $F_{n+1} = F_n + F_{n-1}$ et $F_{n+2} = F_{n+1} + F_n$. Il vient

$$\begin{aligned} F_{n+2}F_n - F_{n+1}^2 &= [F_{n+1} + F_n] \times F_n - [F_n + F_{n-1}] \times F_{n+1} \\ &= F_n^2 - F_{n+1}F_{n-1} \end{aligned}$$

- **Conclusion :** par récurrence, on a montré que

$$\forall n \in \mathbf{N}^\star,\ F_{n+1}F_{n-1} - F_n^2 = (-1)^n.$$

En particulier, en posant pour tout entier $n \in \mathbf{N}^\star$, $U_n = (-1)^n F_{n-1}$, on a obtenu les relations

$$\forall n \in \mathbf{N}^\star, \quad U_{n+1}F_n + U_nF_{n+1} = 1.$$

Le **Théorème de Bezout** permet alors de conclure que pour tout entier naturel $n \in \mathbf{N}^\star$, les nombres de Fibonacci F_n et F_{n+1} sont premiers entre eux.

2. Notons pour $n \in \mathbf{N}$,

$$\mathcal{P}(n) \qquad \forall p \in \mathbf{N}^\star, \qquad F_{n+p} = F_pF_{n+1} + F_{p-1}F_n$$

On montre par récurrence sur n que $\forall n \in \mathbf{N}, \mathcal{P}(n)$.

- **Initialisation :** lorsque $n = 0$, on a bien pour tout entier $p \in \mathbf{N}^\star$ $F_p = F_p \times F_1 + F_0F_{p-1}$ puisque $F_0 = 0$ et $F_1 = 1$.
- **Hérédité :** soit $n \in \mathbf{N}$ tel que $\mathcal{P}(n)$. Considérons un entier $p \in \mathbf{N}^\star$. *A fortiori* $p+1$ est un entier naturel non nul et l'hypothèse de récurrence – qui est en l'occurrence une hypothèse de type universel – appliquée à $p+1$, donne :

$$\begin{aligned} F_{(n+1)+p} &= F_{n+(p+1)} = F_{p+1}F_{n+1} + F_pF_n \\ &= [F_p + F_{p-1}]F_{n+1} + F_pF_n \\ &= F_p \times [F_n + F_{n+1}] + F_{p-1} \times F_{n+1} \\ &= F_pF_{n+2} + F_{p-1}F_{n+1} \end{aligned}$$

- **Conclusion :**par récurrence sur n, on a montré que

Soit $(n,p) \in \mathbf{N} \times \mathbf{N}^\star$. On sait que $F_{n+p} = F_pF_{n+1} + F_{p-1}F_n$ et on montre que $PGCD(F_n, F_p) = PGCD(F_{n+p}, F_p)$. Pour ce faire, on vérifie, par double-inclusion que $\mathcal{D}(F_n, F_p) = \mathcal{D}(F_{n+p}, F_p)$.

- $\subset$ si d divise à la fois F_n et F_p, d'après la relation précédente il divise aussi $F_{n+p} = F_pF_{n+1} + F_{p-1}F_n$. D'où l'on tire que $d \in \mathcal{D}(F_{n+p}, F_p)$.
- $\supset$ si d divise F_p et F_{n+p}. Alors, d'une part d divise aussi $F_{p-1}F_n = F_{n+p} - F_pF_{n+1}$. D'autre part, d divise F_p tandis que F_p et F_{p-1} sont premiers entre eux (d'après la première question), donc d et F_{p-1} sont aussi premiers entre eux. Finalement, d'après le **théorème de Gauss** on peut conclure que d doit diviser F_n. Il s'agit donc bien d'un diviseur commun à F_p et F_n.

Par double-inclusion, on a bien établi que $\mathcal{D}(F_n, F_p) = \mathcal{D}(F_{n+p}, F_p)$. En particulier, ces ensembles ont donc même plus grand élément : $PGCD(F_n, F_p) = PGCD(F_{n+p}, F_p)$

3. Soit $(m,n) \in \mathbf{N}^2$ un couple d'entiers non tous les deux nuls. On suppose sans perte de généralité que $n \neq 0$. Effectuons la division euclidienne de m par n. On a

$$m = nq + r, \text{ où } 0 \leq r \leq n-1$$

En itérant le résultat de la question précédente, on a

$$\begin{aligned} PGCD(F_n, F_r) &= PGCD(F_n, F_{r+n}) = \cdots = PGCD(F_n, F_{r+nq}) \\ &= PGCD(F_n, F_m) \end{aligned}$$

Ainsi, pour tout couple d'entiers naturels non nuls, on a

$$PGCD(F_m, F_n) = PGCD(F_n, F_r),$$

où r est le reste de la division euclidienne de m par n.

Finalement, on conclut à l'aide de l'algorithme d'Euclide pour le calcul de $d = PGCD(m,n)$: si $a_0 \geq a_1 > \cdots > a_m = d > 0$ est la suite des restes non nuls successivement apparus, on a d'après ce qui précède

$$\begin{aligned} PGCD(F_m, F_n) &= PGCD(F_{a_0}, F_{a_1}) \\ &= PGCD(F_{a_1}, F_{a_2}) \\ &\vdots \end{aligned}$$

Problème 1 Convolution de suites réelles

1.a Soit $u,v\in E$. $\forall n\in\mathbb{N},(u\star v)(n)=\sum_{k=0}^{n}u(k)v(n-k)\underset{\ell=n-k}{=}\sum_{\ell=0}^{n}u(n-\ell)v(\ell)=\sum_{k=0}^{n}v(k)u(n-k)=(v\star u)(n)$.

Par suite $u\star v=v\star u$ et on peut conclure que $\star$ est commutative.

Soit $u,v,w\in E$. $\forall n\in\mathbb{N},\big[(u\star v)\star w\big](n)=\sum_{k=0}^{n}(u\star v)(k)w(n-k)=\sum_{k=0}^{n}\sum_{\ell=0}^{k}u(\ell)v(k-\ell)w(n-k)$ et

$\big[u\star(v\star w)\big](n)=\sum_{k=0}^{n}u(k)\sum_{\ell=0}^{n-k}v(\ell)w(n-k-\ell)=\sum_{k=0}^{n}\sum_{\ell=0}^{n-k}u(k)v(\ell)w(n-k-\ell)$.

Pour identifier les deux expressions, plusieurs démarches sont possibles :

(1) $\big[(u\star v)\star w\big](n)=\sum_{p+q+r=n}u(p)v(q)w(r)=\big[u\star(v\star w)\big](n)$.

(2)
$$\big[u\star(v\star w)\big](n)=\sum_{k=0}^{n}\sum_{\ell=0}^{n-k}u(k)v(\ell)w(n-k-\ell)\underset{\ell'=n-k-\ell}{=}\sum_{k=0}^{n}\sum_{\ell'=0}^{n-k}u(k)v(n-k-\ell')w(\ell')$$
$$=\sum_{\ell'=0}^{n}\sum_{k=0}^{n-\ell'}u(k)v(n-k-\ell')w(\ell')\underset{\ell'=n-\ell}{=}\sum_{\ell=0}^{n}\sum_{k=0}^{\ell}u(k)v(\ell-k)w(n-\ell)=\big[(u\star v)\star w\big](n)$$

1.b Soit $u\in E$. $\forall n\in\mathbb{N},(u\star\varepsilon)(n)=\sum_{k=0}^{n}u(k)\varepsilon(n-k)=0+\cdots+0+u(n)=u(n)$ donc $u\star\varepsilon=u$.

Par commutativité, on aussi $\varepsilon\star u=u$ et on peut donc conclure que ε est élément neutre.

1.c Soit $u,v,w\in E$. $\forall n\in\mathbb{N}$ on a :

$$\big[u\star(v+w)\big](n)=\sum_{k=0}^{n}u(k)(v+w)(n-k)=\sum_{k=0}^{n}u(k)(v(n-k)+w(n-k)$$
$$=\sum_{k=0}^{n}u(k)v(n-k)+\sum_{k=0}^{n}u(k)w(n-k)=(u\star v)(n)+(u\star w)(n)=\big[(u\star v)+(u\star w)\big](n)$$

Par suite $u\star(v+w)=(u\star v)+(u\star w)$ et par commutativité : $(v+w)\star u=(v\star u)+(w\star u)$.

Finalement $\star$ est distributive sur $+$.

1.d $(E,+,\star)$ est un anneau commutatif de nulle la suite nulle et d'élément unité la suite ε .

2.a Cherchons $v\in E$ tel que $u\star v=\varepsilon$ i.e. tel que $(u\star v)(0)=1$ et $\forall n\in\mathbb{N}^*,(u\star v)(n)=0$

$(u\star v)(0)=u(0)v(0)=1$ impose $v(0)=1$.

$(u\star v)(1)=u(0)v(1)+u(1)v(0)=v(1)+\rho=0$ impose $v(1)=-\rho$.

$(u\star v)(2)=u(0)v(2)+u(1)v(1)+u(2)v(0)=v(2)-\rho^2+\rho^2=0$ impose $v(2)=0$ et ainsi de suite.

Suite à cette étude nous visualisons quel doit être l'inverse de u , il ne reste plus qu'à vérifier que « ça marche » :

Soit v la suite définie par $v(0)=1$, $v(1)=-\rho$ et $\forall n\geq 2,v(n)=0$.

On a $(u\star v)(0)=u(0)v(0)=1$, $(u\star v)(1)=u(0)v(1)+v(1)u(0)=v(1)+\rho=0$ et $\forall n\geq 2$:

$(u\star v)(n)=\sum_{k=0}^{n}u(k)v(n-k)=0+\cdots+0+\rho^{n-1}\times(-\rho)+\rho^{n}\times 1=0$.

Finalement $u\star v=\varepsilon$ et par commutativité $v\star u=\varepsilon$. Ainsi u est inversible et d'inverse v .

2.b $F\subset E$.

$\varepsilon\in F$ car la suite ε est nulle à partir du rang 1.

Soit $u,v\in F$. Il existe $p,q\in\mathbb{N}$ tel que $\forall n>p,u(n)=0$ et $\forall n>q,v(n)=0$.

D'une part : $\forall n>\max(p,q),(u-v)(n)=0$ et donc $u-v\in F$.

D'autre part : $\forall n>p+q,(u\star v)(n)=\sum_{k=0}^{n}u(k)v(n-k)=\sum_{k=0}^{p}u(k)v(n-k)+\sum_{k=p+1}^{n}u(k)v(n-k)$.

Or $\sum_{k=0}^{p}u(k)v(n-k)=0$ car $\forall k\leq p$ on a $n-k\geq n-p>q$ donc $v(n-k)=0$

et $\sum_{k=p+1}^{n}u(k)v(n-k)=0$ car $\forall k\geq p+1$ on a $u(k)=0$. Ainsi $(u\star v)(n)=0$.

Finalement $u\star v\in F$.

Ainsi F est un sous anneau de $(E,+,\star)$.

2.c Clairement $f(\varepsilon)=\varepsilon$. Soit $u,v\in E$. $\forall n\in\mathbb{N}$ on a

$\big[f(u+v)\big](n)=(-1)^n(u+v)(n)=(-1)^n u(n)+(-1)^n v(n)=\big[f(u)\big](n)+\big[f(v)\big](n)=\big[f(u)+f(v)\big](n)$

Donc $f(u+v)=f(u)+f(v)$.

$$\big[f(u\star v)\big](n)=(-1)^n(u\star v)(n)=(-1)^n\sum_{k=0}^{n}u(k)v(n-k)=\sum_{k=0}^{n}(-1)^k u(k)(-1)^{n-k}v(n-k)$$

donc $\big[f(u\star v)\big](n)=\sum_{k=0}^{n}\big[f(u)\big](k)\big[f(v)\big](n-k)=\big[f(u)\star f(v)\big](n)$

donc $f(u\star v)=f(u)\star f(v)$.

Finalement f est un endomorphisme de l'anneau $(E,+,\star)$.

De plus $\forall u\in E,\forall n\in\mathbb{N}$ on a $\big[f(f(u))\big](n)=(-1)^n f(u)(n)=(-1)^n(-1)^n u(n)=u(n)$ donc $(f\circ f)(u)=u$ puis $f=\mathrm{Id}_E$. Ainsi f est une involution. C'est donc une bijection et on peut alors parler d'automorphisme involutif.

3.a Soit $u\in E$ inversible et v sont inverse.

$u\star v=\varepsilon$ donne $(u\star v)(0)=1$ i.e. $u(0)v(0)=1$. Par suite $u(0)\neq 0$.

3.b Soit $u\in E$ tel que $u(0)\neq 0$. Soit $v\in E$ la suite définie par :

$$v(0)=\frac{1}{u(0)}\text{ et }\forall n\in\mathbb{N}^*,v(n)=-\frac{\sum_{k=1}^{n}u(k)v(n-k)}{u(0)}.$$

Cette suite est correctement définie et on a d'une part $(u\star v)(0)=1$ et d'autre

part $\forall n\in\mathbb{N}^*,(u\star v)(n)=\sum_{k=0}^{n}u(k)v(n-k)=u(0)v(n)+\sum_{k=1}^{n}u(k)v(n-k)=0$ de sorte que $u\star v=\varepsilon$. De plus par commutativité $v\star u=\varepsilon$ et on peut conclure que u est inversible (et d'inverse v).

4.a $\{n\in\mathbb{N}/u(n)\neq 0\}$ est une partie de $\mathbb{N}$ non vide car $u\neq 0$.

Puisque toute partie non vide de $\mathbb{N}$ possède un plus petit élément, l'existence de p est assurée.

De même pour l'existence de q .

4.b $(u\star v)(p+q)=\sum_{k=0}^{p+q}u(k)v(p+q-k)=\sum_{k=0}^{p-1}u(k)v(p+q-k)+u(p)v(q)+\sum_{k=p+1}^{p+q}u(k)v(p+q-k)$.

Or $\sum_{k=0}^{p-1}u(k)v(p+q-k)=0$ car $\forall k\leq p-1$ on a $u(k)=0$,

et $\sum_{k=p+1}^{p+q}u(k)v(p+q-k)=0$ car $\forall k\geq p+1$ on a $p+q-k\leq q-1$ donc $v(k)=0$.

Finalement $(u\star v)(p+q)=u(p)v(q)\neq 0$.

4.c Par le résultat ci-dessus $u\neq 0$ et $v\neq 0\Rightarrow u\star v\neq 0$.

Par contraposée $u\star v=0\Rightarrow u=0$ ou $v=0$.

De plus l'anneau $(E,+,\star)$ est commutatif et non réduit à $\{0\}$, il est donc intègre.

Problème 2 Entiers somme de deux carrés

Partie I

1.a $\mathbb{Z}[i]\subset\mathbb{C}$, $1=1+0.i\in\mathbb{Z}[i]$ et $\forall u,v\in\mathbb{Z}[i]$, on peut écrire $u=a+ib$, $v=c+id$ avec $a,b,c,d\in\mathbb{Z}$
On a $u-v=(a-c)+i(b-d)\in\mathbb{Z}[i]$ (car $a-c,b-d\in\mathbb{Z}$),
et $uv=(ac-bd)+i(ad+bc)\in\mathbb{Z}[i]$ car $ac-bd,ad+bc\in\mathbb{Z}$.
Ainsi $\mathbb{Z}[i]$ est un sous anneau de $(\mathbb{C},+,\times)$.

1.b $\forall u,v\in\mathbb{Z}[i]$, $N(uv)=uv\overline{uv}=u\overline{u}v\overline{v}=N(u)N(v)$
$\forall u\in\mathbb{Z}[i]$, on peut écrire $u=a+ib$ avec $a,b\in\mathbb{Z}$ donc $N(u)=u\overline{u}=a^2+b^2\in\mathbb{N}$.

1.c Supposons $u\in\mathbb{Z}[i]$ inversible et introduisons $v\in\mathbb{Z}[i]$ tel que $uv=1$.
On a $N(uv)=N(1)=1$ et $N(uv)=N(u)N(v)$ donc $N(u)N(v)=1$ avec $N(u),N(v)\in\mathbb{N}$.
Par suite $N(u)=N(v)=1$.
On peut écrire $u=a+ib$ avec $a,b\in\mathbb{Z}$.
$N(u)=a^2+b^2=1$ donne $(a,b)=(1,0),(-1,0),(0,1)$ ou $(0,-1)$ donc $u=\pm1$ ou $u=\pm i$.
Inversement, ses éléments sont inversibles car $1\times1=1$, $(-1)\times(-1)=1$, $i\times(-i)=1$ et $(-i)\times i=1$.
$U=\{1,i,-1,-i\}$.

2.a Si $u\,|\,v$ et $v\,|\,w$ alors il existe $s,t\in\mathbb{Z}[i]$ tel que $v=su$ et $w=tv$.
On a alors $w=(st)u$ avec $st\in\mathbb{Z}[i]$ et par suite $u\,|\,w$.

2.b Si $u\,|\,v$ et $v\,|\,u$ alors il existe $s,t\in\mathbb{Z}[i]$ tel que $v=su$ et $u=tv$.
Par suite $u=(ts)u$.
Si $u\neq0$, on obtient $ts=1$ donc t est inversible et alors $t=\pm1$ ou $t=\pm i$.
Par suite $u=\pm v$ ou $u=\pm iv$.
Si $u=0$ alors $v=su=u$ et donc $u=v$.

2.c Si $u\,|\,v$ alors il existe $s\in\mathbb{Z}[i]$ tel que $v=su$. On a alors $N(v)=N(su)=N(s)N(u)$ avec $N(s)\in\mathbb{N}$
donc $N(u)\,|\,N(v)$.

2.d $N(1+i)=2$ et $\text{Div}(2)\cap\mathbb{N}=\{1,2\}$.
Si u divise $1+i$ alors $N(u)=1$ ou $N(u)=2$.
Si $N(u)=1$ alors $u=\pm1$ ou $u=\pm i$.
Si $N(u)=2$ alors $u=1+i,1-i,-1+i$ ou $-1-i$.
Inversement, les nombres proposés sont diviseurs de $1+i$.
$N(1+3i)=10$ et $\text{Div}(10)\cap\mathbb{N}=\{1,2,5,10\}$.
Si $N(u)=1$ alors $u=\pm1$ ou $u=\pm i$.
Si $N(u)=2$ alors $u=1+i,1-i,-1+i$ ou $-1-i$.
Si $N(u)=5$ alors $u=1+2i,1-2i,-2+i$ ou $-2-i$.
Si $N(u)=10$ alors $u=1+3i,1-3i,-3+i$ ou $-3-i$.
Inversement, les nombres proposés sont diviseurs de $1+3i$.

3.a Soit a et b les entiers respectivement les plus proches de $\text{Re}(z)$ et $\text{Im}(z)$.
Pour $u=a+i.b\in\mathbb{Z}[i]$, on a $N(u-v)=(a-\text{Re}(z))^2+(b-\text{Im}\,z)^2\leq\frac{1}{4}+\frac{1}{4}\leq\frac{1}{2}<1$.
Il n'y a pas unicité de u. Par exemple, pour $z=\frac{1+i}{2}$, les quatre complexes $0,1,i$ et $1+i$ conviennent.

3.b Soit $q\in\mathbb{Z}[i]$ tel que $N\left(q-\frac{u}{v}\right)<1$ et $r=u-vq\in\mathbb{Z}[i]$.

On a $u=vq+r$ et $N(r)=N(u-vq)=N(v)N\left(\frac{u}{v}-q\right)<N(v)$ (sachant $N(v)>0$).

Partie II

1. $\delta.\mathbb{Z}[i]\subset\mathbb{Z}[i]$. $0=\delta.0\in\delta.\mathbb{Z}[i]$. $\forall x,y\in\delta.\mathbb{Z}[i]$, on peut écrire $x=\delta.u$ et $y=\delta.v$ avec $u,v\in\mathbb{Z}[i]$.
On a $x-y=\delta.(u-v)\in\delta.\mathbb{Z}[i]$ car $u-v\in\mathbb{Z}[i]$. Ainsi $\delta.\mathbb{Z}[i]$ est un sous groupe de $(\mathbb{Z}[i],+)$.

2.a $u=u.1+v.0\in I(u,v)$ et $v=u.0+v.1\in I(u,v)$.

2.b $A=\{N(w)/w\in I(u,v)\setminus\{0\}\}$ est une partie de $\mathbb{Z}$, minorée par 1 et non vide car $N(u)$ ou $N(v)$ appartient à cet ensemble (selon que $u\neq 0$ ou $v\neq 0$). Par suite A possède un plus petit élément $d>0$.

2.c $\delta\in I(u,v)$ donc on peut écrire $\delta=u\xi+v\xi'$ avec $\xi,\xi'\in\mathbb{Z}[i]$.
$\forall x\in\delta.\mathbb{Z}[i]$, on peut écrire $x=\delta y$ avec $y\in\mathbb{Z}[i]$.
On a alors $x=u(\delta\xi)+v(\delta\xi')\in I(u,v)$. Ainsi $\delta.\mathbb{Z}[i]\subset I(u,v)$.
Inversement, soit $x\in I(u,v)$. On peut écrire $x=uz+vz'$ avec $z,z'\in\mathbb{Z}[i]$
Réalisons la division euclidienne de x par δ : $x=\delta q+r$ avec $N(r)<N(\delta)$.
Or $r=x-\delta q=u(z-\xi q)+v(z'-\xi' q)\in I(u,v)$ donc si $r\neq 0$, on a $N(r)\in A$. Ceci contredit la définition de $d=\min A$ car $N(r)<N(\delta)=d$. Nécessairement $r=0$ et par suite $x\in\delta.\mathbb{Z}[i]$.

2.d $u\in I(u,v)=\delta.\mathbb{Z}[i]$ donc on peut écrire $u=\delta.z$ avec $z\in\mathbb{Z}[i]$. Ainsi $\delta\mid u$. De même $\delta\mid v$.
Si $w\mid\delta$ alors $w\mid u$ et $w\mid v$ par transitivité de la divisibilité.
Inversement si $w\mid u$ et $w\mid v$ alors on peut écrire $u=ws$ et $v=wt$ avec $s,t\in\mathbb{Z}[i]$ et donc l'écriture $\delta=u\xi+v\xi'$ avec $\xi,\xi'\in\mathbb{Z}[i]$ introduite ci-dessus donne $\delta=w(s\xi+t\xi')$. Ainsi $w\mid\delta$.

3.a $I(u,v)=\delta.\mathbb{Z}[i]=\mathbb{Z}[i]$ car $\delta\in\{\pm 1,\pm i\}$.
Or $1\in\mathbb{Z}[i]$ donc $1\in I(u,v)$ et par suite $\exists z,z'\in\mathbb{Z}[i]$ tels que $1=uz+vz'$.

3.b Supposons $u\mid vw$. On a $w=w\times 1=uwz+vwz'$, or $u\mid uwz$ et $u\mid vwz'$ donc sans difficultés $u\mid w$.

4.a Posons δ un pgcd de u et v. δ est un diviseur de l'élément irréductible u.
Si $\delta=\pm u$ ou $\delta=\pm iu$ alors, puisque $\delta\mid v$, $u\mid v$. Ceci est exclu.
Il reste $\delta=\pm 1$ ou $\delta=\pm i$ et donc u et v sont premiers entre eux.

4.b Si u divise v : ok
Sinon, u est premier avec v et donc puisque $u\mid vw$ on a $u\mid w$ en vertu de II.3b.

Partie III

1.a Si $n\in\Sigma$ alors on peut écrire $n=a^2+b^2$ avec $a,b\in\mathbb{Z}$ et alors $n=N(u)$ avec $u=a+i.b\in\mathbb{Z}[i]$.
Inversement, si $n=N(u)$ avec $u\in\mathbb{Z}[i]$, alors on peut écrire $u=a+i.b$ avec $a,b\in\mathbb{Z}$ et on a $N(u)=a^2+b^2\in\Sigma$.

1.b Si $n,n'\in\Sigma$ alors on peut écrire $n=N(u)$ et $n'=N(v)$ avec $u,v\in\mathbb{Z}[i]$.
On a alors $nn'=N(u)N(v)=N(uv)$ avec $uv\in\mathbb{Z}[i]$ donc $nn'\in\Sigma$.

2.a Puisque p est premier et strictement supérieur à 2, il n'est pas divisible par 2.
Par suite $p\equiv 1$ ou $p\equiv 3$ modulo 4.
Puisque $p\in\Sigma$, on peut écrire $p=a^2+b^2$ avec $a,b\in\mathbb{Z}$.
Or les seuls valeurs possibles de a^2 modulo 4 sont 0 ou 1 donc $p=0$, 1 ou 2 modulo 4.
Compte tenu de ce qui précède, il reste $p=1$ modulo 4.

2.b Si p n'est par irréductible alors on peut écrire $p=uv$ avec $u,v\in\mathbb{Z}[i]\setminus\{\pm1,\pm i\}$.
On a alors $p^2=N(p)=N(u)N(v)$. Puisque $N(u)\neq1$, $N(v)\neq1$ et p premier, on a $N(u)=N(v)=p$ et donc $p\in\Sigma$.

3.a Puisque $p\equiv3$ modulo 4, p n'appartient pas à Σ (via III.2a) et donc p est irréductible (via III.2b)
On a $p\,|\,a^2+b^2=(a+ib)(a-ib)$ or p est irréductible donc $p\,|\,(a+ib)$ ou $p\,|\,(a-ib)$.
Or il est clair que $p\,|\,z\Rightarrow p\,|\,\overline{z}$, donc $p\,|\,(a+ib)$ et $p\,|\,(a-ib)$.

3.b Suite a ce qui précède $p^2\,|\,(a+ib)(a-ib)=n$.
Cette dernière divisibilité a lieu a priori dans $\mathbb{Z}[i]$, mais puisque n/p^2 est le rapport de deux entiers, sera un entier et donc la divisibilité a lieu dans $\mathbb{Z}$.

4. Soit $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_N^{\alpha_N}$ de la forme proposée. $\forall1\leq i\leq N$:
Si $p_i=2$ ou $p_i\equiv1$ modulo 4 alors $p_i\in\Sigma$ (car $2=1^2+1^2$ et par la réciproque admise en III.2a)
Par suite $p_i^{\alpha_i}\in\Sigma$ car Σ est stable par produit (III.1.b)
Si $p_i\equiv3$ modulo 4 alors $\alpha_i=2\beta_i$ et $p_i^{\alpha_i}=p_i^{2\beta_i}=(p_i^2)^{\beta_i}\in\Sigma$ car $p_i^2=p_i^2+0^2\in\Sigma$.
Puisque tous les $p_1^{\alpha_1},\dots,p_N^{\alpha_N}$ appartiennent à Σ, $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_N^{\alpha_N}$ appartient à Σ.
Inversement : Soit $n\in\Sigma\cap\mathbb{N}^*$. Si $n=1$, n est de la forme voulue.
Si $n\geq2$, introduisons sa décomposition primaire $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_N^{\alpha_N}$.
Pour tout $1\leq i\leq N$ tel que $p_i\equiv3$ modulo 4.
Si $\alpha_i=0$ alors α_i est pair.
Si $\alpha_i>0$ alors $p_i\,|\,n$. Ecrivons $n=a^2+b^2$ avec $a,b\in\mathbb{Z}$.
Comme vu en III.3a, on a $p_i\,|\,(a+ib)$ ce qui permet d'écrire $a+ib=p_i(c+id)$.
On a alors $n=p_i^2(c^2+d^2)=p_i^2n'$ avec $n'=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_i^{\alpha_i-2}\dots p_N^{\alpha_N}\in\Sigma$.
On peut alors reprendre la démarche avec n' et, champagne !, α_i est pair.